

AO 106 (Rev. 5/85) Affidavit for Search Warrant

United States District Court

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA

v.

JEFFREY LEE PARSON
a/k/a "Teekid"

WARRANT FOR ARREST

CASE NO. 03-457M

To: The United States Marshal
and any Authorized United States OfficerYOU ARE HEREBY COMMANDED to arrest JEFFREY LEE PARSON
Name

and bring him forthwith to the nearest magistrate to answer a

 Indictment Information XXX Complaint Order of Court Violation Notice Probation
Violation Petition

charging him with (brief description of offense)

Internationally Causing and Attempting to Cause Damage to a Protected Computer

in violation of Title 18 United States Code, Section 1030

MONICA J. BENTON
Name of Issuing Officer[Signature]
Signature of Issuing OfficerU.S. MAGISTRATE JUDGE
Title of Issuing OfficerAugust 28, 2003 at Seattle, Washington
Date and LocationBail fixed at \$ _____ by _____
Name of Judicial Officer

RETURN

This warrant was received and exec
at _____

OPTIONAL FORM 99 (7-80)

000-0000

DATE RECEIVED _____

DATE OF ARREST _____

N2N 7540-01-317-7388

5006-101

GENERAL SERVICES ADMINISTRATION

NATURE OF ARRESTING OFFICER _____

Magistrate Judge Benton

FILED ENTERED
 LODGED RECEIVED

AUG 28 2003

AT SEATTLE
 CLERK U.S. DISTRICT COURT
 WESTERN DISTRICT OF WASHINGTON DEPUTY

I hereby certify that the
 annexed instrument is a true
 and correct copy of the original
 on file in my office.
 ATTEST: BRUCE BENTON
 Clerk, U. S. District Court
 Western District of Washington

Bruce Benton
 Deputy Clerk

UNITED STATES DISTRICT COURT
 WESTERN DISTRICT OF WASHINGTON
 AT SEATTLE

UNITED STATES OF AMERICA,
 Plaintiff,

v.

JEFFREY LEE PARSON,
 Defendant.

MAGISTRATE'S DOCKET NO.
 CASE NO.

03-457M

COMPLAINT FOR VIOLATION
 U.S.C. Title 18,
 Sections 1030(a)(5)(A)(i),
 1030(a)(5)(B)(i), 1030(b), and
 1030(c)(4)(A), and Section 2

BEFORE Monica J. Benton, United States Magistrate Judge,
 United States Courthouse, 1010 Fifth Avenue, Seattle, Washington.

The undersigned complainant being duly sworn states:

COUNT ONE

(Intentionally Causing and Attempting to Cause Damage to a Protected Computer)

Beginning on or about August 2003, and continuing until the present, within the Western District of Washington, and elsewhere, JEFFREY LEE PARSON knowingly caused and attempted to cause the transmission of a program, information, code, and command, that is, an Internet worm and packets of data sent in the form of a distributed denial of service attack, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to protected computers, that is, computers of Microsoft Corporation and other computers throughout the world that were used in interstate or foreign commerce or communication, causing an aggregate loss to Microsoft Corporation and other persons of at least \$5,000 in value during a one-year period.

1 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i),
2 1030(a)(5)(B)(i), 1030(b), and 1030(c)(4)(A), and Section 2.

3 DAVID FARQUHAR, being first duly sworn on oath, deposes and says:

4 1. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States
5 Department of Justice, and have been so employed since February 2003. Before joining the FBI,
6 I was employed in the Information Technologies field for more than five years. During that time
7 I gained experience in web site design, application design and development, database
8 architecture, and data security. I have worked as a Software Consultant, a Senior Database
9 Administrator, and as an Assistant Vice President of Data Management. I am familiar with many
10 different operating systems and web server application software, including Microsoft Windows
11 and its versions, several varieties of Unix and Linux, the Apache web server, and Microsoft's
12 web server named Microsoft Internet Information Server. In addition, I have been involved in
13 internal company investigations and inquiries requiring the examination and evaluation of digital
14 evidence stored on various computer systems. In these investigations and inquiries I was
15 typically responsible for determining: (1) what particular actions a user may have taken; (2) what
16 evidence of this activity may have been created; (3) what evidence was found; and (4) what
17 conclusions regarding the user's activities could be drawn from the evidence found. I am
18 currently assigned to the Cyber Squad in the Seattle Division of the FBI. The Cyber Squad is
19 assigned to investigations involving, among other things, computer intrusions and Internet fraud.

20 2. I make this affidavit in support of a Complaint charging JEFFREY LEE PARSON
21 with Intentionally Causing and Attempting to Cause Damage to Protected Computers, and aiding
22 and abetting, in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i),
23 1030(a)(5)(B)(i), 1030(b), and 1030(c)(4)(A), and Section 2. The information contained in this
24 affidavit is based on my own participation in a joint FBI and United States Secret Service (USSS)
25 investigation into the "Blaster" Internet worm and its variants, as well as information provided to
26 me by other FBI and USSS Special Agents and by the victims, including Microsoft Corporation
27 (Microsoft). I have set forth only the facts that I believe are necessary to establish probable cause
28 for the charges.

1 3. The Internet is a globally distributed network of interconnected computers. Traffic
2 is routed from computer to computer based on Internet Protocol (IP) addresses. IP addresses
3 uniquely identify computers and provide a uniform method of identifying them. Several central
4 organizations manage blocks of addresses which are then leased to smaller companies that resell
5 individual addresses. Because humans often have difficulty remembering long strings of
6 numbers, Internet domain names (e.g., www.fbi.gov) exist to provide simple-to-remember
7 addresses that are resolved, or matched, to the IP addresses of the intended computer. Users can
8 provide a domain name, and services available on the Internet resolve the name to a number and
9 provide a connection to the appropriate IP address. Domain names are registered with several
10 registrant organizations that require that domain names be globally unique. To facilitate Internet
11 based communications, domain name registration and IP address allocation information is
12 publicly available.

13 4. Two types of malicious communications can be directed toward a computer on the
14 Internet, and they can be employed separately or together. The first type of malicious
15 communication seeks to gain unauthorized access or control of the computer remotely. The
16 second type of malicious communication seeks to disrupt the legitimate operation and usage of
17 the computer. This is known as a Denial of Service (DoS) attack. A DoS attack also can be
18 distributed among multiple computers, each conducting its own DoS attack against the same
19 target. In this scenario, the target is inundated with requests from an overwhelming number of
20 sources. The human operators of such a target computer cannot instruct the computer to ignore
21 malicious sources fast enough to prevent the computer from being overwhelmed. This type of
22 attack is called a Distributed Denial of Service (DDoS) attack, and it is much more common than
23 a single-source DoS. A DDoS attack is capable of effectively shutting down a target computer by
24 overwhelming its resources. DDoS attacks prevent an entity (e.g., government agency, business,
25 etc.) from conducting its online business activities, undermine public confidence in the Internet
26 and the entity, and divert entity resources.

27 5. An individual who gains remote control of a computer can use that computer to
28 participate in a DDoS attack. This provides a buffer between the individual launching the attack

1 and the target. The target sees communications from the compromised computer (often referred
2 to as a "drone"), not from the controlling individual. The effectiveness of the DDoS attack is
3 dependent on the number of drone computers and the capacity of the target computer to handle
4 communication requests.

5 6. An individual who compromises other computers for later use as agents in a DDoS
6 attack has options for controlling the attack. The first option is to preprogram the drone computer
7 with instructions on how, where, and when to attack. A second option is to establish a line of
8 communication between the individual and each drone computer. This allows remote control of
9 multiple drone computers. This latter option provides the individual with the ability to adapt and
10 modify the attack at any time.

11 7. As set forth in greater detail below, based on my training and experience, I believe
12 that JEFFREY LEE PARSON is responsible for, among other things, knowingly developing and
13 releasing, and aiding and abetting the development and release of, onto the Internet a variant of
14 the Blaster worm that infected at least 7,000 individual Internet users' computers, turned those
15 computers into drones that attacked or attempted to attack Microsoft and, in particular, its web
16 site www.windowsupdate.com. As a result, JEFFREY LEE PARSON intentionally caused
17 significant damage, without authorization, to Microsoft and other victim computers that
18 significantly exceeds \$5,000.00.

19 8. The information in the following paragraphs was provided to me by representatives
20 of Microsoft, including several software development engineers who have been assigned to work
21 on the issues described herein. Sometime in early July 2003, Microsoft Corporation (Microsoft)
22 was contacted confidentially by a research group known as Last Stage of Delirium (LSD). LSD
23 had found a vulnerability in Microsoft's Windows family of operating system software. The
24 vulnerability allows a computer to issue a command to another computer that will cause an error
25 on the target computer. Following this error, the user issuing the command gains elevated access
26 to the target computer. This allows the attacking computer to gain unauthorized access to the
27 target computer. Microsoft developed a patch that removes the vulnerability and posted the patch
28

1 in Microsoft Security Bulletin MS03-026. This was made available for download from Microsoft
2 on or about July 16, 2003.

3 9. Shortly after the release of the patch, a Chinese group of computer experts named
4 "XFocus" reverse-engineered the patch and found the vulnerability. XFocus then developed
5 exploit code that can be used to exploit the vulnerability and gain remote access to target
6 computers. XFocus also developed a scanning tool that searches the Internet for computers that
7 have the vulnerability and that have not been patched. XFocus made their source code for the
8 exploit and the scanning tool available to the public via the Internet.

9 10. On or about August 11, 2003, Microsoft became aware of an Internet worm named
10 Blaster. Blaster is based on the XFocus code and scans the Internet for targets, attacks them, and
11 installs itself on the target computers. Each target computer then begins scanning and infecting
12 other computers. Within three days, Blaster had infected an estimated one hundred thousand to
13 two hundred thousand computers. By August 15, 2003, estimates were as high as more than one
14 million infected computers. The Blaster worm included a preprogrammed payload of DDoS
15 attack code. The attack code used a date and time based algorithm to launch a DDoS attack
16 against Microsoft's www.windowsupdate.com domain name beginning on August 16, 2003. The
17 Microsoft servers affected by this are located in the Western District of Washington. Despite
18 exposure in the media and from Microsoft, hundreds of thousands, if not millions, of computers
19 have not yet been patched.

20 11. On or about August 14, 2003, Microsoft became aware of several variants of the
21 Blaster code. One particular variant was referred to by the Internet security community by a
22 number of different names including "W32/Lovesan.worm.b" (hereinafter "Lovesan B").
23 Microsoft engineers were able to obtain several copies of executable code for this variant.
24 Microsoft engineers disassembled the code and were able to understand what this variant does.
25 Lovesan B contains a variant of the Blaster worm, renamed "teekids.exe". This variant code is
26 functionally equivalent to the Blaster code, including the code that directs compromised
27 computers to attack the Microsoft domain name www.windowsupdate.com, but it contains some
28 slightly modified message strings. In addition, Lovesan B installs a back door (a way of getting

1 into a password protected system without using the password) on the infected computer. The
2 back door, known as "Lithium", allows remote control of the system. Finally, Lovesan B
3 contacts the web site www.t33kid.com. It then registers itself with a computer script residing on
4 the web site by providing its IP address to the site.

5 12. Microsoft was able to test Lovesan B by intentionally infecting a computer and
6 witnessing it connect to the www.t33kid.com web site and provide its IP address. This was also
7 witnessed by USSS Special Agent John Liao, who has served as an Electronic Crimes Special
8 Agent for five years and has received extensive training on network intrusions and forensic
9 computer data analysis. Based on the above information, Special Agent Liao and Microsoft
10 believe that the www.t33kid.com web site was being used to compile a list of compromised
11 computers. Using the Lithium back door, and the list of computers, all the infected computers
12 can be remotely controlled.

13 13. Subsequently, Special Agent Liao used a Domain Name Service query search on a
14 publicly available database to resolve the web site (www.t33kid.com) to Internet Protocol (IP)
15 Address 209.126.247.158. Special Agent Liao then researched this IP address and discovered
16 that it belongs to California Regional Internet, Inc. (CARI). CARI is located at 8929A Complex
17 Drive, San Diego, California 92123. This information was provided by the American Registry
18 for Internet Numbers (ARIN).

19 14. A closer examination of the www.t33kid.com web site by Special Agent Liao
20 revealed that the web site contained the programming source code for multiple Internet worms.
21 These worms included one peer-to-peer worm that spreads via Kazaa and Imesh file sharing.
22 Also on the web site were multiple links to various other web sites, such as
23 www.evileyesoftware.com, www.bots.bl.am, and www.sinred.com. These web sites offer
24 various back doors that can be downloaded, distributed, and used.

25 15. On August 15, 2003, I contacted Steve Wallace at CARI. He advised that Keith
26 Baldwin's company, SouthO, rents hardware rack space and Internet connectivity from CARI.
27 Wallace confirmed that the IP address 209.126.247.158 is allocated to Keith Baldwin and is
28 physically located at 8929A Complex Drive, San Diego, California 92123.

1 16. On the same day, I contacted Keith Baldwin, and he provided the following
2 information: He provides hardware and leases computer server access to several clients. Brian
3 Davis is the client who leased the IP address 209.126.247.158. Baldwin advised that Davis leases
4 web hosting services on the server to several parties. Baldwin provided the following physical
5 address for Davis: 8248 April Lane, Watauga, Texas 76148. Baldwin stated that he was not
6 surprised that there was some issue with the web site using that IP address because CARI had
7 forwarded to him complaints it had received about the web site. Specifically, Baldwin advised
8 that on August 12, 2003, he received an email from CARI indicating that someone had contacted
9 CARI to complain that his computer had been infected with some code that was attempting to
10 contact the www.t33kid.com web site.

11 17. On August 16, 2003, FBI agents secured the computer that hosted the
12 www.t33kid.com web site and obtained a search warrant for it. The forensic analysis of that
13 computer is pending.

14 18. Also on August 16, 2003, Brian Davis was interviewed at his residence at, 8248
15 April Lane, Watauga, Texas, by USSS Special Agent Derrick Day and FBI Special Agent Miguel
16 Clarke. Davis stated that he controlled the computer located at CARI in San Diego, but did not
17 have anything to do with the web site www.t33kid.com. Davis stated that www.t33kid.com was
18 set-up and operated by a user on his system called "teekid". Davis stated that he had
19 communicated with "teekid" on multiple occasions over Internet Relay Chat (IRC). Davis was
20 able to provide an IP address for "teekid" of 24.94.194.76. Davis stated that he knew "teekid"
21 had performed DoS attacks and had written various Internet worms.

22 19. On August 18, 2003, Special Agent Day informed Special Agent Liao that Brian
23 Davis had contacted him with more supporting information about "teekid". Davis informed
24 Special Agent Day that he had been doing additional research and had discovered a web site that
25 appeared to match the www.t33kid.com web site. Davis identified the newly discovered web site
26 as dl.t33kid.com.

27 20. Upon receiving this information, Special Agent Liao used the ARIN public online
28 database to determine the IP address to which the dl.t33kid.com name is assigned. This research

1 revealed that dl.t33kid.com is linked to the IP address 24.94.194.76, which is the same IP address
2 provided by Brian Davis for "teekid". Therefore, it appears that "teekid" is hosting the
3 dl.t33kid.com web site on his own computer, using the 24.94.194.76 IP address. Special Agent
4 Liau accessed that web site and found that it does indeed match the www.t33kid.com website,
5 which as set forth above had been used for the collection of IP addresses of compromised
6 computers. Since dl.t33kid.com is a copy of www.t33kid.com, it also can be used to capture IP
7 addresses of compromised computers. This list of computers can then be used to perform DDoS
8 or other Internet attacks.

9 21. Also on August 18, 2003, Special Agent Liau used the ARIN public online
10 database on the entire t33kid.com domain name, and found that it is registered to JEFF PARSON,
11 603 8th Ave. S, Hopkins, MN.

12 22. On the same day, Time Warner Cable, an Internet Service Provider, confirmed that
13 from July 1, 2003, to the present, IP address 24.94.194.76 was being used by the account of
14 Robert Parson, 603 8th Ave. S., Hopkins, Minnesota 55343-7730. The account includes the user
15 names "rparson", "grinderrm4", and "teekid". The Internet service provided to that address is via
16 cable or digital subscriber line (DSL). In the case of cable or DSL Internet service, the IP address
17 is assigned to a computer located at the account's physical address.

18 23. On the same day, Special Agent Liau conducted searches on the online database
19 Choicepoint for Robert Parson and JEFF PARSON at the 603 8th Ave. S., Hopkins, MN, address.
20 According to Choicepoint, Robert, Rita, and JEFF PARSON all reside at the address. JEFFREY
21 LEE PARSON, who is 18 years old, also has an identification card issued to him at that address.

22 24. On August 19, 2003, FBI Special Agent Michael Lawrence obtained a search
23 warrant from the United States District Court for the District of Minnesota for the residence at
24 603 8th Ave. S., Hopkins, Minnesota. FBI and USSS Special Agents executed the warrant the
25 same day. As a result of their search, the agents found and seized seven computers located in
26 several rooms in the house. The forensic analysis of these computers is pending.

27 25. At the time of the search, FBI Special Agent Eric Smithmier interviewed JEFFREY
28 LEE PARSON, who provided the following information: PARSON admitted modifying the

1 Blaster worm and creating the variant known by a number of different names including
2 W32/Lovesan.worm.b. PARSON also admitted that he renamed the original "MSBlast.exe"
3 executable "teekids.exe", after his online name "teekid". PARSON explained that he included
4 the back door remote access software "Lithium" so that he could reconnect to the infected
5 computers at a later time. In addition, in order to maintain a list of compromised computers,
6 PARSON admitted that he included code that directed each of the infected computers to contact
7 the www.t33kid.com website and register itself.

8 26. I have spoken with Microsoft representatives about the losses they incurred as a
9 result of the Blaster worm, and in particular the variant that JEFFREY LEE PARSON released on
10 the Internet. Microsoft expended significant internal and external (e.g., contracted) resources to
11 respond to the DDoS attack launched by JEFFREY LEE PARSON. Those resources were used
12 for a number of different purposes directly related to the Blaster worm including, but not limited
13 to, minimizing any damage to Microsoft, conducting damage assessments, restoring full access
14 for its customers to Microsoft resources including, in particular, the patch for the Blaster worm,
15 and the like. The loss to Microsoft significantly exceeds the \$5,000.00 threshold set forth in Title
16 18, United States Code, Section 1030(c)(4)(A). In addition, at least 7,000 individual Internet
17 users' computers were compromised by the variant of the Blaster worm that was released by
18 JEFFREY LEE PARSON. As a result, each of those users had to disinfect their systems resulting
19 in a presently unknown, but significant aggregate loss, to them.

20 //

21 //

22 //

23 //

24 //

25 //

26 //

27 //


28 //

27. Based on the foregoing information, I believe there is probable cause that
JEFFREY LEE PARSON has committed the crime of Intentionally Causing and Attempting to
Cause Damage to a Protected Computer, and aiding and abetting, in violation of Title 18, United
States Code, Section 1030(a)(5)(A)(i) and (B)(i), Section 1030(b), Section 1030(c)(4)(A), and
Section 2.



DAVID FARQUHAR, Complainant
Special Agent, Federal Bureau of Investigation

Complaint and affidavit sworn to before me this 28 day of August, 2003.



MONICA J. BENTON
United States Magistrate Judge

COMPLAINT/PARSON - 10

UNITED STATES ATTORNEY
601 UNION STREET, SUITE 5100
SEATTLE, WASHINGTON 98101-3903
(206) 553-7970

TOTAL P.02